

$(1 - 2u^k)$ -CONSTACYCLIC CODES OVER
 $\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p + u^3\mathbb{F}_p + \cdots + u^k\mathbb{F}_p$

ZAHID RAZA AND AMRINA RANA

ABSTRACT. Let \mathbb{F}_p be a finite field and u be an indeterminate. This article studies $(1 - 2u^k)$ -constacyclic codes over the ring $\mathcal{R} = \mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p + u^3\mathbb{F}_p + \cdots + u^k\mathbb{F}_p$ where $u^{k+1} = u$. We illustrate the generator polynomials and investigate the structural properties of these codes via decomposition theorem.

1. INTRODUCTION

The study of coding theory was initiated by Blake in 1970. Many authors worked on different contexts of codes i.e., Linear codes, cyclic codes, constacyclic codes and etc. The breakthrough work on linear codes was done after remarkable paper of Hammon et.al [?] which showed non-linear binary codes can be constructed from cyclic codes over \mathbb{Z}_4 via its Gray images. So, cyclic code over the finite rings is one of the significant kind of algebraic codes. Constacyclic codes constitute a remarkable generalization of cyclic codes, hence form an important class of linear codes in coding theory. Constacyclic codes have practical applications in engineering, as they can be efficiently encoded using shift registers. They also have rich algebraic structures for efficient error detection and correction which further applies from data networking to satellite communications. There is a vast literature on constacyclic codes over finite fields and their applications for detailed see, [1, 3, 7, 5, 6]. Zhu and Wang investigated $(1 - 2u)$ Constacyclic codes over $\mathbb{F}_p + u\mathbb{F}_p$ where $v^2 = v$ in [7]. Moreover, Yildiz and Karadeniz [2] studied $(1 + v)$ Constacyclic codes of odd length over the ring $\mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p + uv\mathbb{F}_p$.

This present paper is focussed on the class of constacyclic codes over the ring $\mathcal{R} = \mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p + u^3\mathbb{F}_p + \cdots + u^k\mathbb{F}_p$ where $u^{k+1} = u$. It is the natural generalization of the results given by Mostafansab and Karimi on the $(1 - 2u^2)$ -constacyclic codes over the ring $\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p$ in [17]. Let α, β and γ be maps from \mathcal{R}^m to \mathcal{R}^m given by

$$\alpha(s_0, s_1, \dots, s_{m-1}) = (s_{n-1}, s_0, s_1, \dots, s_{m-2})$$

$$\beta(s_0, s_1, \dots, s_{m-1}) = (-s_{m-1}, s_0, s_1, \dots, s_{m-2}) \text{ and}$$

$$\gamma(s_0, s_1, \dots, s_{m-1}) = ((1 - 2u^k)s_{m-1}, s_0, s_1, \dots, s_{m-2})$$

respectively. Let \mathcal{L} be a linear code of length m over \mathcal{R} . Then \mathcal{L} is said to be cyclic if $\alpha(\mathcal{L}) = \mathcal{L}$, negacyclic if $\beta(\mathcal{L}) = \mathcal{L}$ and $(1 - 2u^k)$ -constacyclic if $\gamma(\mathcal{L}) = \mathcal{L}$.

2010 *Mathematics Subject Classification.* Primary 94B05, 94B15; Secondary 11T71, 13M99.

Key words and phrases. Finite fields, cyclic codes, constacyclic codes.

Let \mathcal{L} be a code of length m over \mathcal{R} , and $P(\mathcal{L})$ be its polynomial representation, i.e.,

$$P(\mathcal{L}) = \left\{ \sum_{i=0}^{m-1} s_i a^i \mid (s_0, \dots, s_{m-1}) \in \mathcal{L} \right\}$$

It is easy to see that:

Theorem 1.1. *A code \mathcal{L} of length m over \mathcal{R} is $(1 - 2u^k)$ -constacyclic if and only if $P(\mathcal{L})$ is an ideal of $\mathcal{R}[a]/\langle a^m - (1 - 2u^k) \rangle$.*

Let $x = (a_0, a_1, \dots, a_{m-1})$ and $y = (b_0, b_1, \dots, b_{m-1})$ be two elements of \mathcal{R}^m . The Euclidean inner product of x and y in \mathcal{R}^m is defined as $x \cdot y = a_0 b_0 + a_1 b_1 + \dots + a_{m-1} b_{m-1}$ where the operation is performed in \mathcal{R} . The dual code of \mathcal{L} is defined as $\mathcal{L}^\perp = \{x \in \mathcal{R}^m \mid x \cdot y = 0 \text{ for every } y \in \mathcal{L}\}$.

We define the Gray map $\Phi : \mathcal{R} \rightarrow \mathbb{F}_p^k$ by

$$a_0 + ua_1 + u^2 a_2 + \dots + u^k a_k \mapsto (-a_k, a_1, a_3, \dots, 2a_0 + a_k)$$

This map can be extended to \mathcal{R}^m in a natural way:

$$\Phi : \mathcal{R}^m \rightarrow \mathbb{F}_p^{km}$$

$$(s_0, s_1, \dots, s_{m-1}) \mapsto (-a_k^0, -a_k^1 - \dots - a_k^{m-1}, a_1^0, a_1^1, \dots, a_1^{n-1}, a_3^0, a_3^1, \dots, a_3^{m-1}, \dots, 2a_0^0 + a_k^0, 2a_0^1 + a_k^1, \dots, 2a_0^{m-1} + a_k^{m-1})$$

where $s_i = a_0^i + ua_1^i + u^2 a_2^i + \dots + u^k a_k^i$, $0 \leq i \leq m-1$.

We denote by $\sigma_1, \sigma_2, \sigma_3$, respectively the following elements of \mathcal{R} :

$$\sigma_1 = (1 - u^k), \quad \sigma_2 = 2^{-1}(u^{k-1} + u^k), \quad \sigma_3 = 2^{-1}(-u^{k-1} + u^k)$$

Note that σ_1, σ_2 and σ_3 are mutually orthogonal idempotents over \mathcal{R} and $\sigma_1 + \sigma_2 + \sigma_3 = 1$. Let \mathcal{L} be a linear code of length m over \mathcal{R} . Define

$$\mathcal{L}_1 = \{a \in \mathbb{F}_p^m \mid \exists b, c \in \mathbb{F}_p^m, \sigma_1 a + \sigma_2 b + \sigma_3 c \in \mathcal{L}\}$$

$$\mathcal{L}_2 = \{b \in \mathbb{F}_p^m \mid \exists a, c \in \mathbb{F}_p^m, \sigma_1 a + \sigma_2 b + \sigma_3 c \in \mathcal{L}\}$$

$$\mathcal{L}_3 = \{c \in \mathbb{F}_p^m \mid \exists a, b \in \mathbb{F}_p^m, \sigma_1 a + \sigma_2 b + \sigma_3 c \in \mathcal{L}\}$$

Then $\mathcal{L}_1, \mathcal{L}_2$ and \mathcal{L}_3 are all linear codes of length m over \mathbb{F}_p . Moreover, the code \mathcal{L} of length m over \mathcal{R} can be uniquely expressed as $\mathcal{L} = \sigma_1 \mathcal{L}_1 \oplus \sigma_2 \mathcal{L}_2 \oplus \sigma_3 \mathcal{L}_3$.

2. MAIN RESULTS

Theorem 2.1. *Let γ denote the $(1 - 2u^k)$ -constacyclic shift of \mathcal{R}^m and α be the cyclic shift of \mathbb{F}_p^{km} . If Φ is the Gray map of \mathcal{R}^m into \mathbb{F}_p^{km} , then $\Phi\gamma = \alpha\Phi$.*

Proof. Let $\bar{s} = (s_0, s_1, \dots, s_{m-1}) \in \mathcal{R}^m$ where $s_i = a_0^i + ua_1^i + u^2 a_2^i + \dots + u^k a_k^i$, and $a_0^i, a_1^i, \dots, a_k^i \in \mathbb{F}_p$, for $0 \leq i \leq m-1$. Then taking $(1 - 2u^k)$ -constacyclic shift on \bar{s} , we have

$$\begin{aligned} \gamma(\bar{s}) &= ((1 - 2u^k)s_{m-1}, s_0, s_1, \dots, s_{m-2}) \\ &= (a_0^{m-1} - ua_1^{m-1} - u^2 a_2^{m-1} - \dots, +(-2a_0^{m-1} - a_k^{m-1})u^k, a_0^0 + ua_1^0 + \dots + u^k a_k^0, \\ &\quad a_0^1 + ua_1^1 + \dots + u^k a_k^1, \dots, a_0^{m-2} + ua_1^{m-2} + \dots + u^k a_k^{m-2}). \end{aligned}$$

Now, using the definition of Gray map Φ , we can deduce that

$$\begin{aligned} \Phi(\gamma(\bar{s})) &= (2a_0^{m-1} + a_k^{m-1}, -a_k^0, -a_k^1 - \cdots - a_k^{m-2}, 2a_0^{m-1} + (-2a_0^{m-1} - a_k^{m-1}) \\ &\quad 2a_0^0 + a_k^0, 2a_0^1 + a_k^1, \dots, 2a_0^{m-1} + a_k^{m-1}). \end{aligned}$$

On the other hand,

$$\begin{aligned} \alpha(\Phi(\bar{s})) &= \alpha(-a_k^0, -a_k^1, \dots, a_k^{m-1}, 2a_0^0 + a_k^0, 2a_0^1 + a_k^1, \dots, 2a_0^{m-1} + a_k^{m-1}) \\ &= (2a_0^{m-1} + a_k^{m-1}, -a_k^{m-1}, -a_k^0, -a_k^1, \dots, a_k^{m-1}, 2a_0^0 + a_k^0, 2a_0^1 + a_k^1, \dots, 2a_0^{m-1} + a_k^{m-1}) \end{aligned}$$

Therefore, $\Phi\gamma = \alpha\Phi$. \square

Theorem 2.2. *The Gray image of a $(1 - 2u^k)$ -constacyclic code over \mathcal{R} of length m is a cyclic code over \mathbb{F}_p of length $3m$.*

Proof. Let \mathcal{L} be a $(1 - 2u^k)$ -constacyclic code over \mathcal{R} . Then $\gamma(\mathcal{L}) = \mathcal{L}$. Therefore, $(\Phi\gamma)(\mathcal{L}) = \Phi(\mathcal{L})$. It follows from Theorem 2.1 that $\alpha(\Phi(\mathcal{L})) = \Phi(\mathcal{L})$, which means that $\Phi(\mathcal{L})$ is a cyclic code. \square

Notice that $(1 - 2u^k)^m = 1 - 2u^k$ if m is odd and $(1 - 2u^k)^m = 1$ if m is even.

Proposition 2.3. *Let \mathcal{L} be a code of length m over \mathcal{R} . Then \mathcal{L} is a $(1 - 2u^k)$ -constacyclic code if and only if \mathcal{L}^\perp is a $(1 - 2u^k)$ -constacyclic code.*

Proof. The “only if” part follows from Proposition 2.4 of [3]. For the converse note the fact that $(\mathcal{L}^\perp)^\perp = \mathcal{L}$. \square

Recall that a code \mathcal{L} is said to be self-orthogonal provided $\mathcal{L} \subseteq \mathcal{L}^\perp$.

Proposition 2.4. *Let \mathcal{L} be a code of length m over \mathcal{R} such that $\mathcal{L} \subset (\mathbb{F}_p + u\mathbb{F}_p + u^3\mathbb{F}_p + \cdots + u^k\mathbb{F}_p)^m$. If \mathcal{L} is self-orthogonal, then so is $\Phi(\mathcal{L})$.*

Proof. Assume that \mathcal{L} is self-orthogonal. Let

$$\begin{aligned} s_1 &= (a_0^1 + ua_1^1 + u^3a_3^1 + \cdots + u^ka_k^1) \\ s_2 &= (a_0^2 + ua_1^2 + u^3a_2^2 + \cdots + u^ka_k^2) \in \mathcal{L} \end{aligned}$$

where $a_0^i, a_1^i, a_3^i, \dots, a_k^i \in \mathbb{F}_p^m$ for $i = 1, 2$. Now by Euclidean inner product of s_1 and s_2 , we have

$$\begin{aligned} s_1 \cdot s_2 &= (a_0^1 + ua_1^1 + u^3a_3^1 + \cdots + u^ka_k^1) \cdot (a_0^2 + ua_1^2 + u^3a_2^2 + \cdots + u^ka_k^2) \\ &= (a_0^1a_0^2 + (a_0^1a_1^2 + a_1^1a_0^2 + \cdots + a_k^1a_1^2)u + (a_1^1a_1^2 + \cdots + a_k^1a_k^2)u^2 + \\ &\quad (a_0^1a_3^2 + a_1^1a_3^2 + \cdots + a_k^1a_5^2)u^3 + \cdots + (a_0^1a_k^2 + a_1^1a_k^2 + \cdots + a_k^1a_0^2)u^k \end{aligned}$$

if $s_1 \cdot s_2 = 0$, then

$$\begin{aligned} a_0^1a_0^2 &= (a_0^1a_1^2 + a_1^1a_0^2 + \cdots + a_k^1a_1^2) = (a_0^1a_3^2 + a_1^1a_3^2 + \cdots + a_k^1a_5^2) \\ &= (a_0^1a_k^2 + a_1^1a_k^2 + \cdots + a_k^1a_0^2). \end{aligned}$$

Therefore

$$\begin{aligned} \Phi(s_1) \cdot \Phi(s_2) &= (-a_k^1, a_1^1, a_3^1, \dots, 2a_0^1 + a_k^1) \cdot (-a_k^2, a_1^2, \dots, 2a_0^2 + a_k^2) \\ &= 4a_k^1a_k^2 + a_1^1a_1^2 + a_3^1a_3^2 + \cdots + 2(a_k^1a_k^2 + a_0^1a_k^2 + a_0^2a_k^1). \end{aligned}$$

Hence $\Phi(\mathcal{L}^\perp) \subseteq \Phi(\mathcal{L})^\perp$. Consequently $\Phi(\mathcal{L}) \subseteq \Phi(\mathcal{L})^\perp$. \square

Theorem 2.5. *Let $\mathcal{L} = \sigma_1\mathcal{L}_1 \oplus \sigma_2\mathcal{L}_2 \oplus \sigma_3\mathcal{L}_3$ be a code of length m over \mathcal{R} . Then \mathcal{L} is a $(1 - 2u^k)$ -constacyclic code of length m over \mathcal{R} if and only if \mathcal{L}_1 is cyclic and $\mathcal{L}_2, \mathcal{L}_3$ are negacyclic codes of length m over \mathbb{F}_p .*

Proof. First of all, notice that

$$(1 - 2u^k)\sigma_1 = \sigma_1,$$

$$(1 - 2u^k)\sigma_2 = -\sigma_2,$$

$$(1 - 2u^k)\sigma_3 = -\sigma_3,$$

Let $\bar{s} = (s_0, s_1, \dots, s_{m-1}) \in \mathcal{L}$. Then $s_i = \sigma_1 a_i + \sigma_2 b_i + \sigma_3 c_i$ where $a_i, b_i, c_i \in \mathbb{F}_p$ $0 \leq i \leq m-1$. Let

$$a = (a_0, a_1, \dots, a_{m-1}),$$

$$b = (b_0, b_1, \dots, b_{m-1}),$$

$$c = (c_0, c_1, \dots, c_{m-1}).$$

Then $a \in \mathcal{L}_1$, $b \in \mathcal{L}_2$ and $c \in \mathcal{L}_3$. Assume that \mathcal{L}_1 is cyclic and $\mathcal{L}_2, \mathcal{L}_3$ are negacyclic codes. Therefore $\alpha(a) \in \mathcal{L}_1$, $\beta(b) \in \mathcal{L}_2$ and $\gamma(c) \in \mathcal{L}_3$. Thus $\gamma(\bar{s}) = \sigma_1\alpha(a) + \sigma_2\beta(b) + \sigma_3\gamma(c) \in \mathcal{L}$. Consequently \mathcal{L} is a $(1 - 2u^k)$ -constacyclic codes over \mathcal{R} .

For the converse, let

$$a = (a_0, a_1, \dots, a_{m-1}) \in \mathcal{L}_1,$$

$$b = (b_0, b_1, \dots, b_{m-1}) \in \mathcal{L}_2,$$

$$c = (c_0, c_1, \dots, c_{m-1}) \in \mathcal{L}_3.$$

Set $s_i = \sigma_1 a_i + \sigma_2 b_i + \sigma_3 c_i$ where $0 \leq i \leq m-1$. Hence $\bar{s} = (s_0, s_1, \dots, s_{m-1}) \in \mathcal{L}$. Therefore $\gamma(\bar{s}) = \sigma_1\alpha(a) + \sigma_2\beta(b) + \sigma_3\gamma(c) \in \mathcal{L}$ which shows that $\alpha(a) \in \mathcal{L}_1$, $\beta(b) \in \mathcal{L}_2$ and $\gamma(c) \in \mathcal{L}_3$. So \mathcal{L}_1 is cyclic and $\mathcal{L}_2, \mathcal{L}_3$ are negacyclic codes. \square

Theorem 2.6. *Let $\mathcal{L} = \sigma_1\mathcal{L}_1 \oplus \sigma_2\mathcal{L}_2 \oplus \sigma_3\mathcal{L}_3$ be a $(1 - 2u^k)$ -constacyclic code of length m over \mathcal{R} such that $h_1(a), h_2(a)$ and $h_3(a)$ are the monic generator polynomials of $\mathcal{L}_1, \mathcal{L}_2$ and \mathcal{L}_3 respectively. Then $\mathcal{L} = \langle \sigma_1 h_1(a), \sigma_2 h_2(a), \sigma_3 h_3(a) \rangle$ and $|\mathcal{L}| = p^{3m - \sum_{i=1}^3 \deg(h_i)}$*

Proof. By Theorem 2.5,

$$\mathcal{L}_1 = \langle h_1(a) \rangle \subseteq \mathbb{F}_p[a]/\langle a^m - 1 \rangle, \mathcal{L}_2 = \langle h_2(a) \rangle \subseteq \mathbb{F}_p[a]/\langle a^m + 1 \rangle$$

$$\mathcal{L}_3 = \langle h_3(a) \rangle \subseteq \mathbb{F}_p[a]/\langle a^m + 1 \rangle$$

Since

$$\mathcal{L} = \sigma_1\mathcal{L}_1 \oplus \sigma_2\mathcal{L}_2 \oplus \sigma_3\mathcal{L}_3$$

then

$$\mathcal{L} = \{l(x) | l(x) = \sigma_1 g_1(a) + \sigma_2 g_2(a) + \sigma_3 g_3(a), g_1(a) \in \mathcal{L}_1, g_2(a) \in \mathcal{L}_2 \text{ and } g_3(a) \in \mathcal{L}_3\}.$$

Hence

$$\mathcal{L} \subseteq \langle \sigma_1 h_1(a), \sigma_2 h_2(a), \sigma_3 h_3(a) \rangle \subseteq \mathcal{R}_m = \mathcal{R}[a]/\langle a^m - (1 - 2u^k) \rangle.$$

Suppose that

$$\sigma_1 h_1(a)k_1(a) + \sigma_2 h_2(a)k_2(a) + \sigma_3 h_3(a)k_3(a) \in \langle \sigma_1 h_1(a), \sigma_2 h_2(a), \sigma_3 h_3(a) \rangle$$

where $k_1(a), k_2(a), k_3(a) \in \mathcal{R}_m$. There exist

$$q_1(a) \in \mathbb{F}_p[a]/\langle a^m - 1 \rangle, q_2(a) \in \mathbb{F}_p[a]/\langle a^m + 1 \rangle$$

and $q_3(a) \in \mathbb{F}_p[a]/\langle a^m + 1 \rangle$ such that

$$\sigma_1 k_1(a) = \sigma_1 q_1(a)$$

$$\sigma_2 k_2(a) = \sigma_2 q_2(a)$$

and $\sigma_3 k_3(a) = \sigma_3 q_3(a)$. Therefore

$$\langle \sigma_1 h_1(a), \sigma_2 h_2(a), \sigma_3 h_3(a) \rangle \subseteq \mathcal{L}.$$

Consequently $\mathcal{L} = \langle \sigma_1 h_1(a), \sigma_2 h_2(a), \sigma_3 h_3(a) \rangle$. On the other hand

$$|\mathcal{L}| = |\mathcal{L}_1| \cdot |\mathcal{L}_2| \cdot |\mathcal{L}_3| = p^{3m - \sum_{i=1}^3 \deg(h_i)}.$$

□

Theorem 2.7. *Let \mathcal{L} be a $(1 - 2u^k)$ -constacyclic code of length m over \mathcal{R} . Then there exists a unique polynomial $h(a)$ such that $\mathcal{L} = \langle h(a) \rangle$ where $h(a) = \sigma_1 h_1(a) + \sigma_2 h_2(a) + \sigma_3 h_3(a)$.*

Proof. Suppose that $h_1(a), h_2(a)$ and $h_3(a)$ are the monic generator polynomials of $\mathcal{L}_1, \mathcal{L}_2$ and \mathcal{L}_3 respectively. By Theorem 2.6, we have $\mathcal{L} = \langle \sigma_1 h_1(a), \sigma_2 h_2(a), \sigma_3 h_3(a) \rangle$. Let $h(a) = \sigma_1 h_1(a) + \sigma_2 h_2(a) + \sigma_3 h_3(a)$. Then clearly, $\langle h(a) \rangle \subseteq \mathcal{L}$. On the other hand $\sigma_1 h_1(a) = \sigma_1 h(a)$, $\sigma_2 h_2(a) = \sigma_2 h(a)$ and $\sigma_3 h_3(a) = \sigma_3 h(a)$, whence $\mathcal{L} \subseteq \langle h(a) \rangle$. Thus $\mathcal{L} = \langle h(a) \rangle$. The uniqueness of $h(a)$ is followed by that of $h_1(a), h_2(a)$ and $h_3(a)$. □

Lemma 2.8. *Let $a^m - (1 - 2u^k) = h(a)k(a)$ in $\mathcal{R}[a]$ and let \mathcal{L} be the $(1 - 2u^k)$ -constacyclic code generated by $h(a)$. If $g(a)$ is relatively prime with $k(a)$, then $\mathcal{L} = \langle h(a)k(a) \rangle$.*

Proof. The proof is similar to that of [2, Lemma 2]. □

Theorem 2.9. *Let $\mathcal{L} = \sigma_1 \mathcal{L}_1 \oplus \sigma_2 \mathcal{L}_2 \oplus \sigma_3 \mathcal{L}_3$ be a $(1 - 2u^k)$ -constacyclic code of length m over \mathcal{R} such that $h_1(a), h_2(a)$ and $h_3(a)$ are the monic generator polynomials of $\mathcal{L}_1, \mathcal{L}_2$ and \mathcal{L}_3 respectively. Suppose that*

$$h_1(a)k_1(a) = a^m - 1,$$

$$h_2(a)k_2(a) = h_3(a)k_3(a) = a^m + 1,$$

and set $h(a) = \sigma_1 h_1(a) + \sigma_2 h_2(a) + \sigma_3 h_3(a)$, $k(a) = \sigma_1 k_1(a) + \sigma_2 k_2(a) + \sigma_3 k_3(a)$. Then

- (1) $h(a)k(a) = a^m - (1 - 2u^k)$.
- (2) If $\text{GCD}(g_i(a), k_i(a)) = 1$ for $1 \leq i \leq 3$, then $\text{GCD}(g(a), k(a)) = 1$ and $h(a) = h(a)g(a)$ where $g(a) = \sigma_1 g_1(a) + \sigma_2 g_2(a) + \sigma_3 g_3(a)$.

Proof. (1) By assumptions we have

$$\begin{aligned}
h(a)k(a) &= h(a)(\sigma_1 k_1(a) + \sigma_2 k_2(a) + \sigma_3 k_3(a)) \\
&= \sigma_1 h_1(a)k_1(a) + \sigma_2 h_2(a)k_2(a) + \sigma_3 h_3(a)k_3(a) \\
&= \sigma_1(a^m - 1) + \sigma_2(a^m + 1) + \sigma_3(a^m + 1) \\
&= (\sigma_1 + \sigma_2 + \sigma_3)a^m - (\sigma_1 - \sigma_2 - \sigma_3) \\
&= a^m - (1 - 2u^k).
\end{aligned}$$

Hence, $h(a)k(a) = a^m - (1 - 2u^k)$.

(2) Suppose that $GCD(g_i(a), k_i(a)) = 1$ for $1 \leq i \leq 3$ and let

$$g(a) = \sigma_1 g_1(a) + \sigma_2 g_2(a) + \sigma_3 g_3(a)$$

Then for every $1 \leq i \leq 3$ there exist $u_i(a), v_i(a) \in \mathcal{R}[a]$ such that $u_i(a)g_i(a) + v_i(a)k_i(a) = 1$. Now, set $u(a) := \sigma_1 u_1(a) + \sigma_2 u_2(a) + \sigma_3 u_3(a)$ and $v(a) := \sigma_1 v_1(a) + \sigma_2 v_2(a) + \sigma_3 v_3(a)$. Notice that $\sigma_1 + \sigma_2 + \sigma_3 = 1$, $\sigma_i^2 = 1$ and $\sigma_i \sigma_j = 0$ for every $1 \leq i \neq j \leq 3$. Thus

$$\begin{aligned}
u(a)g(a) + v(a)k(a) &= \sigma_1[u_1 g_1(a) + v_1(a)k_1(a)] + \sigma_2[u_2(a)g_2(a) + v_2(a)k_2(a)] \\
&\quad + \sigma_3[u_3(a)g_3(a) + v_3(a)k_3(a)] = \sigma_1 + \sigma_2 + \sigma_3 = 1.
\end{aligned}$$

It follows that $GCD(g(a), k(a)) = 1$. Now, by part (1) and Lemma 2.8,

$$\mathcal{L} = \langle h(a)g(a) \rangle$$

So, the uniqueness of $h(a)$ implies that $h(a) = h(a)g(a)$. □

Similar to [12, Theorem 3], we have the following theorem.

Theorem 2.10. *Let \mathcal{L} be a $(1 - 2u^k)$ -constacyclic code of length m over \mathcal{R} . Then*

$$\mathcal{L}^\perp = \sigma_1 \mathcal{L}_1^\perp \oplus \sigma_2 \mathcal{L}_2^\perp \oplus \sigma_3 \mathcal{L}_3^\perp.$$

As a consequence of the previous theorems and [14, Theorem 3.3] we have the next result.

Corollary 2.11. *Let $\mathcal{L} = \langle \sigma_1 h_1(a), \sigma_2 h_2(a), \sigma_3 h_3(a) \rangle$ be a $(1 - 2u^k)$ -constacyclic code of length m over \mathcal{R} and $h_1(a), h_2(a)$ and $h_3(a)$ be the monic generator polynomials of $\mathcal{L}_1, \mathcal{L}_2$ and \mathcal{L}_3 respectively. Suppose that $h_1(a)k_1(a) = a^m - 1$ and $h_2(a)k_2(a) = h_3(a)k_3(a) = a^m + 1$ and let $k(a) = \sigma_1 k_1(a) + \sigma_2 k_2(a) + \sigma_3 k_3(a)$. then the following conditions hold:*

- (1) $\mathcal{L}^\perp = \langle \sigma_1 k_1^\perp(a), \sigma_2 k_2^\perp(a), \sigma_3 k_3^\perp(a) \rangle$ and $|\mathcal{L}^\perp| = p^{\sum_{i=1}^3 \deg(h_i)}$
- (2) $\mathcal{L}^\perp = \langle k^\perp(a) \rangle$, $k^\perp(a) = \sigma_1 k_1^\perp(a) + \sigma_2 k_2^\perp(a) + \sigma_3 k_3^\perp(a)$

where for $1 \leq i \leq 3$, $k_i^\perp(a)$ is the reciprocal polynomial of $k_i(a)$, and $k^\perp(a)$ is the reciprocal polynomial of $k(a)$.

Theorem 2.12. *Let $\mu : \mathcal{R}[a]/\langle a^m - 1 \rangle \rightarrow \mathcal{R}[a]/\langle a^m - (1 - 2u^k) \rangle$ be defined as*

$$\mu(l(a)) = l((1 - 2u^k)a)$$

If m is odd, then μ is a ring isomorphism.

Proof. Suppose that $u(a) \equiv v(a) \pmod{a^m - 1}$. Then there exists $k(a) \in \mathcal{R}[a]$ such that $u(a) - v(a) = (a^m - 1)k(a)$. Therefore

$$\begin{aligned} a((1 - 2u^k)a) - b((1 - 2u^k)a) &= ((1 - 2u^k)^m a^m - 1)k((1 - 2u^k)a) \\ &= ((1 - 2u^k)a^m - (1 - 2u^k)^2)k((1 - 2u^k)a) \\ &= (1 - 2u^k)(a^m - (1 - 2u^k))k((1 - 2u^k)a) \end{aligned}$$

which means if $u(a) \equiv v(a) \pmod{a^m - 1}$, then

$$\begin{aligned} u((1 - 2u^k)a) &\equiv v((1 - 2u^k)a) \\ &\pmod{a^m - (1 - 2u^k)} \end{aligned}$$

Now, assume that

$$\begin{aligned} u((1 - 2u^k)a) &\equiv v((1 - 2u^k)a) \\ &\pmod{a^m - (1 - 2u^k)}. \end{aligned}$$

Then there exists $q(a) \in \mathcal{R}[a]$ such that

$$u((1 - 2u^k)a) - v((1 - 2u^k)a) = (a^m - (1 - 2u^k))q(a).$$

Hence

$$\begin{aligned} u(a) - v(a) &= u((1 - 2u^k)^2 a) - v((1 - 2u^k)^2 a) \\ &= ((1 - 2u^k)^m a^m - (1 - 2u^k))q((1 - 2u^k)a) \\ &= ((1 - 2u^k)a^m - (1 - 2u^k))q((1 - 2u^k)a) \\ &= (1 - 2u^k)(a^m - 1)q((1 - 2u^k)a) \end{aligned}$$

which means if $u((1 - 2u^k)a) \equiv v((1 - 2u^k)a) \pmod{a^m - (1 - 2u^k)}$, then $u(a) \equiv v(a) \pmod{a^m - 1}$. Consequently $u(a) \equiv v(a) \pmod{a^m - 1} \Leftrightarrow u((1 - 2u^k)a) \equiv v((1 - 2u^k)a) \pmod{a^m - (1 - 2u^k)}$. Note that one side of the implication tells us that μ is well defined and the other side tells us that it is injective, but since the rings are finite this proves that μ is an isomorphism. \square

Corollary 2.13. *Let m be an odd natural number. Then I is an ideal of*

$$\mathcal{R}[x]/\langle a^m - 1 \rangle$$

if and only if $\mu(I)$ is an ideal of

$$\mathcal{R}[a]/\langle a^m - (1 - 2u^k) \rangle.$$

Corollary 2.14. *Let μ be the permutation of \mathcal{R}^m with m odd such that*

$$\bar{\mu}(d_0, d_1, \dots, d_{n-1}) = (d_0, (1 - 2u^k)d_1, (1 - 2u^k)^2 d_2, \dots, (1 - 2u^k)^i d_i, \dots, (1 - 2u^k)^{m-1} d_{m-1})$$

and \mathcal{D} be a subset of \mathcal{R}^n . Then \mathcal{D} is a cyclic code if and only if $\bar{\mu}(\mathcal{D})$ is a $(1 - 2u^k)$ -constacyclic code.

Definition 2.15. Let ψ be the following permutation of $\{0, 1, \dots, 2m - 1\}$ with m odd:

$$\psi = (1, m + 1)(3, m + 3) \cdots (2i + 1, m + 2i + 1) \cdots (m - 2, 2m - 2)$$

The Nechaev permutation is the permutation ϱ of \mathbb{F}_p^{3m} defined by

$$\varrho(d_0, d_1, \dots, d_{2m-1}) = (d_{\psi(0)}, d_{\psi(1)}, \dots, d_{\psi(2m-1)})$$

Proposition 2.16. *Let μ be defined as above. If ϱ is the Nechaev permutation and m is odd, then $\Phi\bar{\mu} = \varrho\Phi$.*

Proof. Let $\bar{s} = (s_0, s_1, \dots, s_i, \dots, s_{m-1}) \in \mathcal{R}^m$ where $s_i = a_o^i + ua_1^i + u^2a_2^i + \dots + u^ka_k^i$, $0 \leq i \leq m-1$. From

$$\bar{\mu}(\bar{s}) = (s_0, (1 - 2u^k)s_1, \dots, (1 - 2u^k)^i s_i, \dots, (1 - 2u^k)^{m-1} s_{m-1}),$$

it follows that

$$\begin{aligned} (\varrho\bar{\mu})(\bar{r}) = & (-a_k^0, 2a_0^1 + a_k^1, -a_k^2, 2a_0^3 + a_k^3, \dots, 2a_0^{n-2} + a_k^{n-2}, -a_k^{n-1}, a_0^1, a_1^1, \\ & 2a_0^0 + a_k^0, -a_1^1, \dots, a_1^k, a_3^0, a_3^1, \dots, a_3^k, 2a_0^2 + a_k^2, \dots, -a_k^{n-2}, 2a_0^{n-1} + a_k^{n-1}) \end{aligned}$$

is equal to $(\varrho\Phi)(\bar{r})$. \square

Corollary 2.17. *Let ϱ be the Nechaev permutation and m be an odd. If λ is the Gray image of a cyclic code over \mathcal{R} , then $\varrho(\lambda)$ is a cyclic code.*

Proof. Let λ be such that $\lambda = \Phi(\mathcal{D})$ where \mathcal{D} is a cyclic code over \mathcal{R} . From Proposition 2.16, $(\Phi\bar{\mu})(\mathcal{D}) = (\varrho\Phi)(\mathcal{D}) = \pi(\lambda)$. We know from Corollary 2.14 that $\bar{\mu}(\mathcal{D})$ is a $(1 - 2u^k)$ -constacyclic code. Thus $(\Phi\bar{\mu})(\mathcal{D}) = \pi(\lambda)$ is a cyclic code, by Theorem 2.2. \square

Recall that two codes \mathcal{L}_1 and \mathcal{L}_2 of length m over \mathcal{R} are said to be equivalent if there exists a permutation w of $\{0, 1, \dots, m-1\}$ such that $\mathcal{L}_2 = \bar{w}(\mathcal{L}_1)$ where \bar{w} is the permutation of \mathcal{R}^m such that

$$\bar{w}(d_0, d_1, \dots, d_i, \dots, d_{m-1}) = (d_{w(0)}, d_{w(1)}, \dots, d_{w(i)}, \dots, d_{w(m-1)}).$$

Corollary 2.18. *The Gray image of a cyclic code over \mathcal{R} of odd length is equivalent to a cyclic code.*

Example 2.19. Let $m = 7$ and $a^7 - 1 = (a - 1)(a^3 + a + 1)(a^3 + a^2 + 1)$ in $\mathcal{R}[a]$. Applying the ring isomorphism μ , we have

$$a^7 - (1 - 2u^k) = (a - (1 - 2u^k))(a^3 + a + (1 - 2u^k))(a^3 + (1 - 2u^k)a^2 + (1 - 2u^k)).$$

Let $f_1 = a - (1 - 2u^k)$ and $f_2 = a^3 + a + (1 - 2u^k)$. If $\mathcal{L} = (f_1 f_2)$, then by Theorem 2.2, we know that the Gray image of the $(1 - 2u^k)$ -constacyclic code \mathcal{L} is a cyclic code.

REFERENCES

- [1] M. C. Amarra and F. R. Nemenzo, On $(1 - u)$ -cyclic codes over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$, App. Math. Lett. **21** (2008), 1129-1133.
- [2] N. Aydin, S. Karadeniz and B. Yildiz, Some new binary quasi-cyclic codes from codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, App. Algebra Eng. Commun. Comp., **24** (2013), 355-367.
- [3] H. Q. Dinh, Constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, J. Algebra, **324** (2010), 940-950.
- [4] X. Kai, S. Zhu and L. Wang, A family of constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, J. Syst. Sci. Comp. **25**(2012), 1032-1040.
- [5] Z. O. Ozger, U. U. Kara and B. Yildiz, Linear, cyclic and constacyclic over $S_4 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$, Filomat **28**(2014), 897-906.

- [6] H. Yu, S. Zhu and X. Kai, $(1 - uv)$ -constacyclic codes over $\mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p + uv\mathbb{F}_p$, *J. Syst. Sci. Comp.* **27**(2014), 811-816.
- [7] Sh. Zhu and L. Wang, A class of constacyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$ and its Gray image, *Disc. Math.* **311** (2011), 2677-2682.
- [8] A. Bonnecaze and P. Udaya, Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$, *IEEE Trans. Inf. Theory*, **45** (1999), 1250-1255.
- [9] H. Q. Dinh, Constacyclic codes of length 2^s over Galois extension rings of $\mathbb{F}_2 + u\mathbb{F}_2$, *IEEE Trans. Inf. Theory*, **55** (2009), 1730-1740.
- [10] H. Q. Dinh, Negacyclic codes of length 2^s over Galois rings, *IEEE Trans. Inf. Theory*, **51** (2005), 4252-4262.
- [11] H. Q. Dinh and S. R. López-Permouth, Cyclic and negacyclic codes over finite chain rings, *IEEE Trans. Inf. Theory*, **50** (2004), 1728-1744.
- [12] J. Gao, Some results on linear codes over $\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p$, *J. Appl. Math. Comput.* **47** (2015), 473-485.
- [13] A. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Sole, The \mathbb{Z}_4 linearity of Kerdock, Preparata, Goethals and related codes, *IEEE Trans. Inf. Theory*, **40** (4) (1994), 301-319.
- [14] S. Jitman, S. Ling and P. Udomkavanich, Skew constacyclic codes over finite chain rings, *Adv. Math. Commun.* **6**(1) (2012), 39-63.
- [15] A. Kaya, B. Yildiz and I. Siap, New extremal binary self-dual codes of length 68 from quadratic residue codes over $\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p$, *Finite Fields Appl.* **29** (2014), 160-177.
- [16] Y. Liu, M. Shi and P. Sole, Quadratic residue codes over $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$, *WAIFI 2014, LNCS* 9061, pp. 204-211.
- [17] A. Mostafansab and N. Karimi, $(1 - 2u^2)$ -constacyclic codes over $\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p$, *arXiv*: 1506.07273
- [18] F. J. MacWilliams and N. J. A. Sloane, *The theory of error correcting codes*, North Holland, 1977.
- [19] J. F. Qian, L. N. Zhang and S. X. Zhu, $(1 + u)$ -cyclic and cyclic codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2$, *Appl. Math. Letters*, **19** (2006), 820-823.
- [20] P. Udaya and A. Bonnecaze, Decoding of cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$, *IEEE Trans. Inf. Theory*, **45** (1999), 2148-2157.

Zahid Raza
Department of Mathematics,
College of Sciences,
University of Sharjah,
P. O. Box 27272 UAE.
Email: zraza@sharjah.ac.ae

Amrina Rana
Department of Mathematics,
National University of Computer and Emerging Sciences,
P. O. Box 54700, Lahore, Pakistan.
Email: amrina.rana.1@gmail.com